BUILDING BLOCK

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DERIVED PIV CREDENTIALS

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of derived personal identity verification (PIV) credentials through collaboration with members of the information technology (IT) community, including vendors of cybersecurity solutions. This sheet provides an overview of the background and challenge, goals, and proposed solution. For more information, see the white paper *Derived Personal Identity Verification (PIV) Credentials* on the NCCoE website. The solution we propose is not the only one available in a fast-moving cybersecurity technology market. If you would like to propose an alternative architecture or know of products that might be applicable to the challenge we are attempting to address, please contact us at piv-nccoe@nist.gov.

BACKGROUND

Organizations protect their information systems, in part, by limiting access to the minimum set of users required to perform a function. This principle of "least privilege" requires both authentication and authorization processes. Federal Information Processing Standards (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, recommends using smart cards with user data in conjunction with passwords to provide two-factor authentication to federal information systems. The standard set in FIPS Publication 201-2 addresses requirements for initial identity proofing, infrastructures to support interoperability of identity credentials, and accreditation of organizations and processes issuing PIV credentials. These credentials are intended to authenticate individuals who require access to federally controlled facilities, information systems, and applications. However, with the emergence of a newer generation of computing devices such as tablets, convertible computers, and in particular mobile devices, the use of PIV-enabled smart cards has proved challenging.

THE CHALLENGE

In 2005, when FIPS 201 was first published, logical access was geared toward traditional computing devices such as desktop and laptop computers. However, enterprises today rely heavily on the productivity of mobile devices (i.e., smartphones and tablets) that do not easily accommodate card readers. Organizations reliant on smart-card-and-password two-factor authentication need to authenticate users of mobile devices in a way that is more tamper-resistant than a password and as easy to use as a smart card. However, it is challenging to use a smart card on the various mobile devices due to their form factor. Attaching or tethering a separate external smart card reader to mobile phones or tablets creates usability and portability challenges and makes the card an impractical authentication token. In addition, some of the modern use case scenarios require the devices to be "on" all the time and the user to quickly authenticate to the system using a personal identification number (PIN).

GOALS

The Derived PIV Credentials project will build on NIST Special Publication 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, to demonstrate how derived smart card credentials can be added to mobile devices so that they can be used for remote authentication to information technology systems in operational environments. National Institute of Standards and Technology (NIST) Interagency Report 8055 details a proof-of-concept prototype platform for use of derived identity credentials in a mobile environment. Although the PIV program and the proof-of-concept focus on federal credentials, personal identity verification and identity-based security in mobile environments are important in both public and private sectors. The NCCoE is initiating the Derived PIV Credentials project to develop and demonstrate extensions from the current platform to a platform that supports both government and private sector applications. To address real-world business challenges, the resulting example solution will be composed of open-source and commercially available components.

LEARN MORE ABOUT NCCOE
Visit http://nccoe.nist.gov

CONTACT US
nccoe@nist.gov
301-975-0200

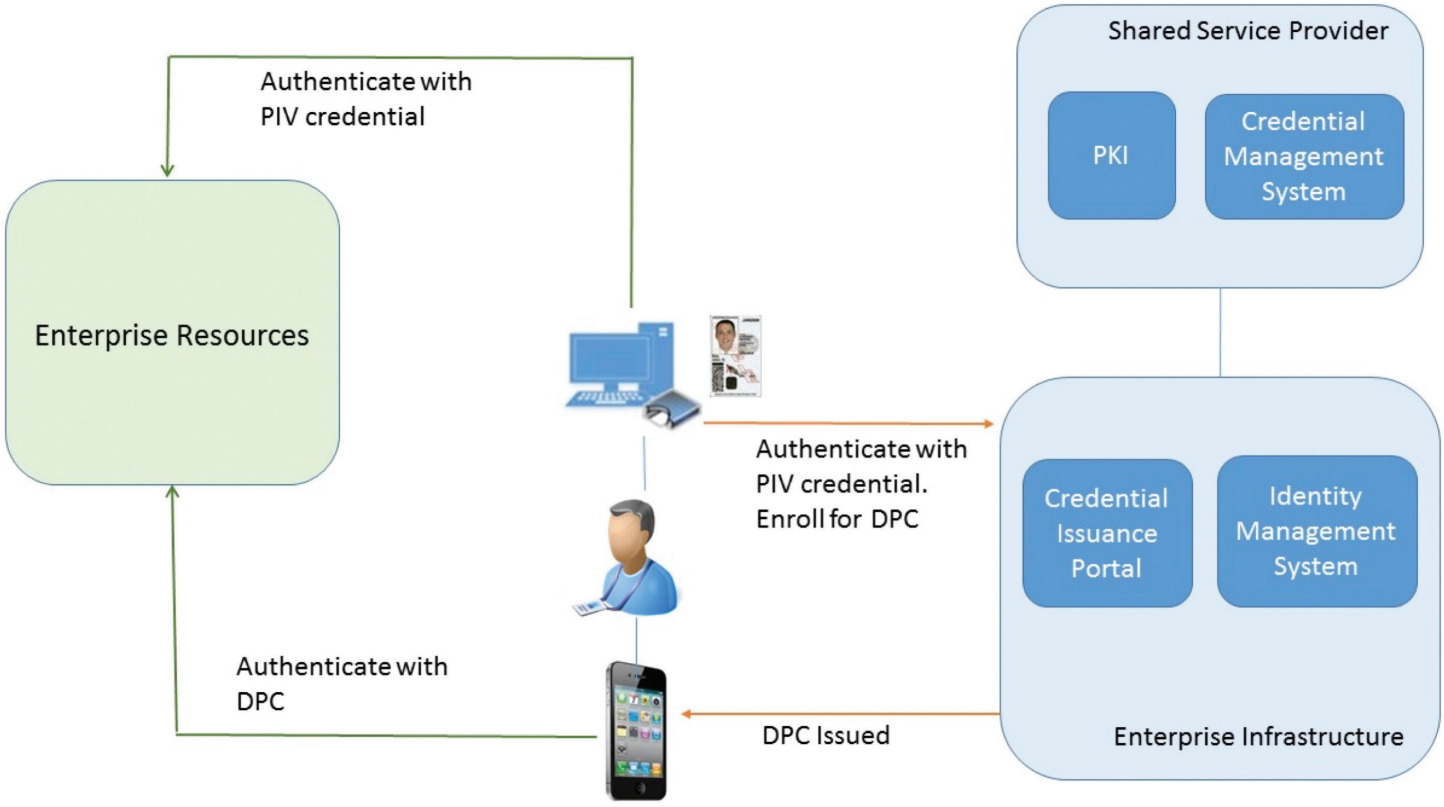
BENEFITS

The goal of this building block effort is a feasible security platform based on Federal PIV standards and an NCCoE-developed demonstration prototype that can support operations in:

- Federal (PIV) infrastructure
- Non-federal critical infrastructure (PIV-Interoperable or PIV-I)
- General business (PIV-Compatible or CIV) environments

For users, this type of security platform allows strong authentication to access web sites and exchange secure email from mobile devices. For organizations, it offers cost savings by incorporating the user's previously established PIV identity into the new derived PIV credential, thereby eliminating the need for further identity proofing.

ARCHITECTURE



HOW TO PARTICIPATE

As a private-public partnership, we are always seeking collaborators, insights, and expertise from businesses, the public, and technology vendors. If you are interested in contributing or collaborating on this project, please contact us at piv-nccoe@nist.gov.

For more information on this project, visit https://nccoe.nist.gov/projects/building_blocks/piv_credentials